REMARKS

Reconsideration and further examination is respectfully requested.

Rejections under 35 U.S.C. §103

Claims 1, 3, 5-12, 18-21, 26-36 and 48-65 were rejected under 35 U.S.C. §103(a) as being unpatentable over Ballardie in view of Bird ("The KryptoKnight Family of Light-Weight Protocol for Authentication and key Distribution...")

Ballardie:

Ballardie proposes a solution to multi-cast key distribution issues, in particular using a Core Based Tree (CBT) protocol. At pages 8-11, Ballardie discloses a group access control mechanism which is illustrated in Figure 1, and includes the steps of a host requesting an authorization stamp from an Authorization Server (AS). The host, upon authorization, receives the Authorization Stamp. The Authorization stamp includes the digital signature *of the AS*. Upon receiving the authorization stamp, the host sends the authorization stamp and an IGMP membership report to the Designated Router (DR). The receiving DR sends a router request to the associated group and an AS in the group responds to the router request. The AS verifies that the digital signature in the authorization stamp matches its own signature (page 9, first paragraph). If it matches, then the DR adds the group to its interface group list.

The present invention is easily distinguished from Ballardie. While Ballardie describes the use of a Certification Authority, which forwards digital signatures of a group of AS to

connecting hosts for the host to include in join requests, in contrast the present invention provides an authentication key *which is unique to the particular host* to the host that seeks to join the shared tree. The unique authentication key is also forwarded to the rendezvous point which forms the root of the tree. While Ballardie's AS compares an authorization stamp against *its own* digital signature, the rendezvous point of the present invention compares the unique authentication key for the host against a previously stored authentication key associated with the host to validate the *particular host*. The authentication system of Ballardie does not include such capabilities of unique host validation; rather, as described in Ballardie, Ballardie authenticates on a general sub-net level. In fact, it is envisioned that the security of the Ballardie system may easily be breached by an unauthorized host who gains access to the AS signature, since the AS of Ballardie does not actually authenticate the particular host. Although Ballardie attempts to narrow down the particular host path by considering which interface port the request is sent on, it would not appear that the system of Ballardie would have the reliability of the present invention.

Applicants note that the Examiner relies on Bird as teaching a two way authentication with tag field. Applicants have amended the claims of the present invention to remove the limitation of the claimed tag including a nonce field, as it is clear to the Applicant that such a limitation is not necessary to distinguish the present invention over the art. Applicants respectfully submit that Bird, which deals with two-way authentication, does nothing to overcome the inadequacies of Ballardie with regard to the claimed invention.

In response to Applicant's previous remarks regarding the distinction between Ballardie and the claimed invention, the Examiner stated, in the office action of February 15, 2006 that:

"... Applicant contends that Ballardie is fundamentally different than the claimed invention .... However, Ballardie teaches that the tree joining process is secure. On page 10,

Ballardie disclose the tree joining process is secure by digitally signing the message will inherently requiring an authentication key in order to verify whether the message has been altered. Furthermore, on page 2, second paragraph, Ballardie discloses "the secure joining implies the provision for authentication ... the scheme we describe provides for the authentication of tree nodes (routers) and receivers (end-systems) as part of the joining process. Key distribution (optional) is an integral part of secure joining..." Therefore, Ballardie does teach authentication key being distributed in order to ensure the transmission of the joined message is secure..."

While Ballardie may disclose a message for secure joining, it is noted that prior art must teach the limitations *as claimed* in order to support a rejection. While Ballardie teaches a tree joining process is secure, it is clear that the method used is fundamentally different from the claimed invention. As described above, Ballardie distributes the AS digital signature to hosts, and performs a comparison of the AS digital signature at the AS when the membership report is received from the DR. While Ballardie mentions the work 'key' it is also clear that authentication keys are not used in the manner claimed by Ballardie. In fact it is noted that Ballardie states, at page 6 "... It is possible to use a separate SAID for each sender of multicast traffic, but this has serious scaling drawbacks..." Applicants would respectfully submit that such language teaches away from a system such as that claimed.

Accordingly, for at least the reason that the combination of references fails to describe or suggest several elements of the claim 1, and further because Ballardie essentially teaches away from the invention as claimed, it is respectfully requested that the rejection be withdrawn.

Independent claims 20, 22, 29, 32, 48, 53, 58 and 65

Each of the independent claims has been amended to recite that the authentication key is uniquely associated with the host device, and further detail that the rendezvous point authenticates the host device by comparing the unique authentication key against a stored key associated with the host device. No such structure is shown or suggested by Ballardie or Bird, either alone or in combination. " Accordingly, for at least this reason Applicant submits that the independent claims are patentably distinct over Ballardie and Bird In addition, their respective dependent claims are patentable for at least the same reasons as their parent independent claims.

Conclusion:

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone the undersigned, Applicants' Attorney at 978-264-6664 so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully submitted,

__July 2, 2007___
Date

___/Lindsay G. McGuinness/_____
Lindsay G. McGuinness, Reg. No. 38,549
Attorney/Agent for Applicant(s)
McGuinness & Manaras LLP
125 Nagog Park
Acton, MA 01720
(978) 264-6664

Docket No. 120-244
Dd: 5/28/2007